IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

BASECAP ANALYTICS, INC. Plaintiff, v. ROBERT AMENN, Defendant.	Civ. No. 1:23-cv-9370(MKV) **JURY TRIAL DEMANDED**

FORENSIC SEARCH PROTOCOL

Pursuant to the Order of this Court (Dkt. 42), the parties shall proceed under the following the Forensic Search Protocol herein.

1. **INTRODUCTION**.
   a. This is a protocol for gathering relevant data from Defendant Robert Amenn's ("Defendant") laptop in such a manner that protects the security of any information gathered and avoids exposure of information not relevant to the Plaintiff, its confidential information, trade secrets or claims in this action.
   b. Archer Hall will serve as the forensic consultant in this matter (hereafter "the Examiner").
2. **SUBJECT OF INSPECTION.**
   a. Defendant represented at the November 21, 2023, preliminary injunction hearing (the "Hearing") that there are no other devices in his possession other than one laptop in his home that he used to perform work for Plaintiff or to store BaseCap information. Defendant will certify under penalty of perjury that this is the device which he will provide for examination and that shall be subject to Inspection under this Protocol (the "Laptop").
   b. In the event that (i) Defendant's representations as stated at the Hearing are inaccurate, (ii) Defendant locates other devices or accounts containing BaseCap

information,[1] or (iii) forensic examination of the Laptop reveals that Defendant transferred BaseCap information to any other devices or accounts, BaseCap reserves the right to return to the Court to secure a separate order or potential protocol delineating how such additional media, devices and/or accounts could be searched for Confidential Information as defined by the parties' NDIAA.

3. **SEARCH OF LAPTOP.** The Court has directed a forensic analysis of the Laptop. Any data collected from the Laptop will be subject to this Protocol.

4. **SEARCH TERMS.** The parties have agreed to a list of keyword search terms. designed to locate information related to this action, attached hereto as Exhibit A (hereafter the "Agreed Upon Search Terms"). These search terms shall be run against the entire physical hard drive of the Laptop, including all unallocated space.

5. **FORENSIC PROCESS.** The search will be conducted for all activity, documents, and information created, edited, modified, accessed or deleted from August 14, 2019 to the Present. The search will involve the following steps:

   a. Searching for Agreed Upon Search Terms in any active (non-deleted) files on the Laptop.

   b. Searching for Agreed Upon Search Terms in deleted files on the Laptop. Deleted files will be searched in the manner outlined for unallocated space.

   c. Searching for the Agreed Upon Search Terms in any communication such as email and messaging applications including but not limited to Teams, Discord, Outlook, FTP, chat applications, etc. on the Laptop using Magnet Axiom, DT Search, Excel, and other tools as Archer Hall determines are necessary to conduct their examination. To be considered "external," the location where the file is sent must be a non-BaseCap source. All email will be subject to the process outlined in 6(e).

   d. Searching for evidence that files with the Agreed Upon Search Terms have been moved from the Laptop to any cloud storage or external storage device using Magnet Axiom, DT Search, Excel, and other tools as Archer Hall determines are necessary to conduct their examination.

---

[1] BaseCap information would be limited to information found by applying the Agreed Upon Search Terms, as defined by Section 4.

e. Allocated, unallocated and slack space will all be searched on the Laptop, in the manner set forth in section 6(c).

6. **METHOD OF COLLECTION.** BaseCap and Defendant will split the cost of renting an office or other space in the state of Washington for up to three days (hereafter "the Rented Space"). A camera will be placed in the Rented Space to monitor all activity therein, which will be paid for by BaseCap and set up by the Examiner with remote supervision from BaseCap Counsel and the Defendant. Data will be collected in the following manner:

a. PRESERVATION – On the first day, the Examiner will preserve a forensic image of the Laptop in Defendant's presence. The image will be encrypted wherein a key is created that is only provided to Defendant; the next day Defendant will bring the key back to the Rented Space so that processing may be done. Defendant agrees not to tamper with the key in any manner or with the Rented Space, and agrees to sign a certification under penalty of perjury attached hereto as Exhibit B, stating that he has not altered or tampered with the Laptop or Archer Hall equipment remotely or in any other manner, nor interfered with any of the steps detailed in this protocol, since January 25, 2024. In the event the examination or any steps delineated herein cannot be performed in the Rented Space, BaseCap reserves the right to return to the Court to secure a separate order or potential protocol for retrieving all Confidential Information as defined in the parties' NDIAA from the Laptop should Defendant not agree to a collection at an alternative location.

b. APPLICATION IDENTIFICATION – The Examiner will open the image and look at the installed applications in the standard installation folders, program files, and program files (x86) folders, and as documented in all registry hives.

c. PROCESSING – On the second day, the Examiner will decrypt the image and process the forensic image to create a searchable index of files, calculate cryptographic hashes of all files, and extract recoverable deleted content. Allocated space on the Laptop will be indexed first ("First Index"). Unallocated space will be indexed next if analysis of allocated space confirms transfer of BaseCap files ("Second Index") to a source not owned or controlled by BaseCap. Slack space will be indexed in both the First and Second Indexes.

d. FORENSIC ANALYSIS – After indexing is complete, the Examiner will search the index for files responsive to the Agreed Upon Search Terms, extracting and preserving the responsive files, analyzing the file-system artifacts to determine last access to the responsive files and dates of access to removable USB devices. Defendant can watch the entire search process in the Rented Space, while Plaintiff attends remotely by virtual meeting platform. All analysis will be limited to what is outlined in section 5 of this protocol.

e. POTENTIAL DISPUTES – In the event that a dispute arises during the examination, the parties will jointly contact Judge Lehrburger. In the event Judge Lehrburger is not available to adjudicate any dispute, the parties will contact the Judge assigned to Part I that day. The Examiner will announce the general, high-level steps (e.g., "preservation"; "encryption"; "review of installed applications"; "decryption" of image; "processing of image"; "indexing"; and "search and extraction") being taken at the beginning of those steps. The Examiner is not required to go into more detail.

f. REVIEW OF FILES AND ACTIVITY –

i. Files. Both sides will receive the list of files and other data including but not limited to emails and chat that were keyword responsive ("the List"), except that the emails ("Emails") will be provided to Defendant first as detailed in section 2 below:

1. As to the List, Defendant will have 14 days, beginning on the day he receives the List, to (a) identify files he believes are not related to BaseCap, its business or its clients and (b) prepare an affidavit declaring why these files do not actually relate to BaseCap, its business or its clients. BaseCap Counsel will then have 14 days, beginning on the day it receives Defendant's affidavit, to review such files and affidavit. If BaseCap Counsel agrees that files do not relate to BaseCap, its business or its clients, such files will be destroyed, otherwise they will be retained for use in this litigation. Any disagreement between the parties as to whether or not certain

files are related to BaseCap, its business or its clients will be brought to the Court's attention for resolution.

2. As to Emails, Defendant will receive the Emails first. Defendant will have 3 days, beginning on the day he receives the Emails, to identify any he believes disclose legal advice or strategies related to pending or anticipated litigation against BaseCap ("Litigation Emails"). Emails identified by Defendant as Litigation Emails will then be submitted to the Court for an *in camera* review to determine whether such emails should be withheld or produced to BaseCap.

ii. Activity. Both parties will get a copy of the activity uncovered by the analysis.

g. The Defendant's hard drive will be wiped clean by The Forensic Consultant after the analysis is complete.

7. CONCLUSION OF INSPECTION.

a. Once the search is completed and only items related to the Agreed Upon Search Terms are extracted, the Forensic Consultant will place the extracted data on an encrypted, password protected USB drive. The Forensic Consultant will then forensically wipe the media containing the forensic image, ensuring that no data is retrievable.

b. All extracted data will be designated as HIGHLY CONFIDENTIAL under the protective order to be entered in this matter, and treated as such until such order is entered. No extracted data may be filed publicly on any court docket or disclosed to third parties unless and until a protective order is entered, in compliance with such protective order.

c. A copy of all extracted data other than emails claimed to be Litigation Emails by Defendant will be provided to Plaintiff and such data may be accessed at times to be agreed upon by the parties by Defendant using a program such as Relativity without any ability to copy, print, transmit or download any such documents, for purposes solely related to litigating this action. Defendant may not screenshot, manually copy, or otherwise capture any extracted data, and a

log will be maintained of files viewed, dates, times and duration of Defendant's viewing of such information. After the court rules on access to Litigation Emails, any such emails permitted by the Court to be produced to Plaintiff will be produced to Plaintiff.

d. A copy of any report generated from the Forensic Analysis will be provided to both parties.

e. At the end of the analysis, the Forensic Consultant will permanently destroy all data from this case, fragments of data, or residual data.

8. **INADVERTENT PRODUCTION.** Inadvertent or unintentional production of documents, information, or material subject to the attorney-client privilege, the work product doctrine, or any other applicable privilege, doctrine, or immunity shall not be deemed a waiver in whole or in part of a claim for confidential treatment. Any party in possession of documents, information, or material subject to the attorney-client privilege, the work product doctrine, or any other applicable privilege, doctrine, or immunity shall immediately destroy such material as soon as reasonably possible after it becomes aware of the privileged nature of the information.

9. **ATTORNEYS' EYES ONLY.** Any non-BaseCap files or information during the forensic examination will be marked as "HIGHLY CONFIDENTIAL" and may only be disclosed to: (i) outside counsel for Plaintiff; and (2) outside consultants or experts (*i.e.*, not existing employees or affiliates of any party to this proceeding).

IT IS SO ORDERED:

Dated: February 15, 2024

HONORABLE ROBERT W. LEHRBURGER
UNITED STATES MAGISTRATE JUDGE